New DNA based dynamical S-Box for block cipher

ABSTRACT

DNA based technique has grown rapidly among researchers in introducing the latest network security algorithms, which can enhance the strength of the current cryptosystem. DNA-based techniques are able to provide a high degree of cryptography algorithm. This article discusses a new DNA based Dynamical S-Box for the symmetric keys block ciphers. The DNA based Dynamical S-Box is proposed using a polynomial calculation in producing an unknown DNA sequences of {A,C,G,T} in mapping the S-Box table in the form of metric [16x16]. The National Institute of Technology and Technology (NIST) 15 Test is used to verify the cipher for this DNA based Dynamical S-Box. However, S-Box testing criteria have been used to verify the crypto security vulnerabilities by the new DNA based Dynamical S-Box. The simulated end result shows that the proposed DNA based Dynamical S-Box can provide a good level of safety after the NIST Randomness Test shows the value is random.

Keyword: Block cipher; AES; Biology chemistry; DNA; S-Box; NIST